REMARKS/ARGUMENTS

Reconsideration and withdrawal of the rejections of the application are respectfully requested in view of the amendments and remarks herewith, which place the application into condition for allowance. The present amendment is being made to facilitate prosecution of the application.

I. STATUS OF THE CLAIMS AND FORMAL MATTERS

Claims 1-28 are currently pending. Claims 1, 17 and 21 are independent. Claim 25-28 are added. Claims 1, 2, 6, 12 and 17-24and are hereby amended. Dependent claims 2, 6, 12, 18-20 and 22-24 are amended to provide consistency of claim language. No new matter has been introduced.

Changes to the claims are not made for the purpose of patentability within the meaning of 35 U.S.C. §101, §102, §103, or §112. Rather, these changes are made simply for clarification and to round out the scope of protection to which Applicants are entitled.

II. REJECTIONS UNDER 35 U.S.C. §102

Claims 1, 10, 11, 16, 17 and 21 were rejected under 35 U.S.C. §102(e) as allegedly anticipated by U.S. Patent No. 6,829,634 to Holt et al. (hereinafter, merely Holt). Applicatns respectfully traverse this rejection.

Independent claim 1, as amended, is representative, and recites, *inter alia*:

> "detecting a <u>manipulation of data</u> in said received message, said manipulation of data <u>changing the outcome of processing</u> by the peer system; and
> . . .

sending a manipulated data alert message . . .message identifying the sending peer responsible for the manipulation of data . . ." (emphases added)

As understood by the Applicants, Holt discloses a technique for broadcasting data across a network. An originating participant sends data to another participant, which in turn sends the data that it receives from a neighbor participant to its other neighbor participants. The computer that originates a message to be broadcast sends that message its neighbors. When a computer receives a message, it sends the message to its other neighbors. Each computer on the broadcast channel, except the originating computer, will receive a copy of each broadcast message from each of its neighbors. Holt uses the redundancy of the message sending to ensure the overall reliability of the broadcast channel. Col. 7, line 55 to col. 8, line 16.

In contrast, claim 1 recites, "detecting a manipulation of data in said received message, said manipulation of data changing the outcome of processing by the peer system; and . . . sending a manipulated data alert message . . .message identifying the sending peer responsible for the manipulation of data . . ." Thus, in one implementation, the peer-to-peer relay network supports the detection of cheating violations that involve the manipulation of data to change an outcome in the processing of online activity, such as to affect the course of a game. Manipulation of the data causing security violations involves unauthorized data or improper use of data to damage the grid or cause the grid to fail. Published Application par. [0155] and FIG. 27

[0157] The peer receives a message from each of its connected peers. A peer will receive the same message through each of its connections with other peers. For example, if a peer has three open connections, the peer receives the same message three times from three respective peers. If a manipulation of the message has occurred, the peer sends a data manipulation alert message. The data manipulation alert message indicates that a violation, such as a cheating violation, has occurred and which peer is responsible for the violation. The peer sends the data manipulation alert message to the connected peers to relay the alert throughout the grid. In another implementation, the peers send the cheating alert to the server for appropriate handling. Published Application pars. [158-159] and FIG. 27.

In an example, the peer can detect a manipulation of the data by comparing the messages received from each of the connected peers. For example, the peer compares the data portion of the message received from each of the other connected peers. The peer determines if the data portion of the message is different for any of the received messages. If the data portion for a message received from one connected peer is different from the data portion for the same message received from the other connected peers, the peer determines that a data manipulation or cheating violation, has occurred. The peer also determines that the one peer that sent the message with the different data is responsible for the cheating violation. Alternatively, the peer can use a different technique to detect a cheating violation or identify the peer responsible for the cheating violation. The peer does not relay the message having a different data portion, if appropriate.

This is distinguishes the present invention from Holt.

Claim 1 is patentable over Holt because that reference does not disclose each and every limitation recited in the claim. In particular, Holt does not disclose, "detecting a manipulation of data in said received message, said manipulation of data changing the outcome of processing by the peer system; and. . . sending a manipulated data alert message . . .message identifying the sending peer responsible for the manipulation of data . . ." as recited in claim 1.

For reasons similar or somewhat similar to those described above with regard to independent claim 1, independent claims 17 and 21 are also believed to be patentable.

III. REJECTIONS UNDER 35 U.S.C. §103

Claims 2-9, 12-15, 18-20 and 22-24 were rejected under 35 U.S.C. §103(a) as allegedly unpatentable over Holt in view of U.S. Published Patent No. 20030229779 of Morais et al. (hereinafter, merely "Morais").

Claims 2-9, 12-15, 18-20 and 22-24 each depend from one of independent claims 1, 17 and 21 and, thus, are believed patentable for at least the same reasons. Morais does not teach or suggest the element missing from Holt as discussed above.

IV. NEW CLAIMS

Claims 25 and 26 add features for detection of a data manipulation violation. In claim 25, a peer system detects a data manipulation violation by comparing the message received from a sending peer to the same message received from other peers connected to the peer-to-peer network. In claim 26, the peer system send back the received message to the sending peer. The sending peer system identifies a peer responsible for a dàta manipulation violation by comparing the send-back message from the peer to the message sent by the sending peer.

Claims 27 and 28 add features for the peer-to-peer relay network to recover from a data manipulation violation. In claim 27, messages from the sending peer responsible for the manipulation of data are ignored. In claim 28, the sending peer responsible for the manipulation of data is forced to disconnect from the peer-to-peer relay network

CONCLUSION

Claims 1-28 are in condition for allowance. In the event the Examiner disagrees with any of statements appearing above with respect to the disclosure in the cited reference, or references, it is respectfully requested that the Examiner specifically indicate those portions of the reference, or references, providing the basis for a contrary view.

Please charge any additional fees that may be needed, and credit any overpayment, to our Deposit Account No. 50-0320.

In view of the foregoing amendments and remarks, it is believed that all of the claims in this application are patentable and Applicants respectfully request early passage to issue of the present application.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: ______________________
Paul A. Levy
Reg. No. 45,748
(212) 588-0800